Manage Vulnerabilities (VULN) Capability Defect False Positives Guide

18 May 2015

Defect False Positive Condition Descriptions

Condition	Description
Desired State Process	A defect false positive condition that occurs when the desired state data is not synchronized, inaccurate, or incomplete. This condition is often the result of manual processes.
Architecture and Sensor Deployment	A defect false positive condition that occurs when an actual state sensor is unable to collect necessary data or communicate with the actual state collection manager (ASCM) due to a poor design, network configurations, sensor collection/reporting limitations, or sensor failures. A defect false positive condition that occurs when the collection system is not updated with the collected and reported data due to poor design, configuration issues, or collector failures.
Data Integrity	A defect false positive condition that occurs when tools and systems providing the actual state data have inconsistencies in how they collect, report, and store the data. This condition also occurs if there is a failure in the data storage mechanism.

VULN Defects

#	Description
VULN-1	Device has vulnerable software product installed
VULN-2	Vulnerable software listing does not contain up-to-date CVE or local vulnerability data
VULN-3	An important data element of the vulnerable software listing or alternative mitigation specification is missing
VULN-4	Vulnerable software cannot be reported within a set timeframe for a device (Non-reporting for Vulnerabilities)

VULN Defect Mapping to False Positive Conditions

	Desired State Process	Architecture and Sensor Deployment	Data Integrity
VULN-1			X
VULN-2	X		
VULN-3	X		
VULN-4		X	